Office of Program Evaluation and Government Accountability (OPEGA)
Response from the Office of Information Technology (OIT)
March 1, 2013
BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY

Executive outline

- Definitions - business continuity, disaster recovery
- Disaster examples
- Industry best practices
- State of Maine current environment
- Future state and timeline

Business Recovery / Disaster Recovery Goals (2013 - 2014)

- Hire full-time DR manager
- Conduct annual DR/ BC test
- Investigate 3rd party cloud solution
- Prevent or mitigate major losses to:
  - Data centers
  - Network
  - Other core infrastructure such as data storage
  - Critical business application systems
  - Critical office locations

Required investment

- Hire, assign an OIT DR manager
- Dedicated Agency BC / DR resources
- Dual data center redundancy with hardware and software (price TBD)
- Networking redundancy for load balancing and fail-over (price TBD)
- 3rd party, independent assessment
- Possible partnership with 3rd party to provide DR services (TBD)

Timeframe (summary):

Mid-2013	End of 2013	End of 2014	Annually
• OIT hire BC/DR manager	• Begin documenting DR exercises (internal and external hosted)	• Independent, 3rd party assessment of readiness and approach. • Subject to availability of funds, complete planning and framework for annual DR exercises of mission-critical systems (internal and external hosted) • First mock disaster drill. • Possible cloud vendor contracts. • BIA of all critical business application systems completed and refreshed.	• Partner with Agencies to develop budget for DR • Annual DR exercises, subject to availability of funds

Section 2: Definitions and Disaster Event Examples

Definitions:

What is a Business Continuity Plan (BCP)?

Business Continuity (BC) is recovery of business processes and operations. BC planning covers how an organization sustains all critical business functions. BC planning ensures maintenance, stability, and recoverability of business functions during and after a disaster. Business Continuity is about business processes and operations; technology (DR) is a subset of BC.

What is Disaster Recovery?

Disaster Recovery (DR) is physical and technology recovery. Disaster Recovery is part of the overall continuity plan that focuses on the technical side of the business, including components such as data backup and recovery.

Time to Recover:

Time to recover business-critical functions and supporting physical and technology infrastructure depends on the level of investment:

- **High investment:** Critical business functions never go down because there is full redundancy at a "hot" alternate site. (Gold standard)
- **Moderate investment:** Critical business functions are recoverable within a few hours or days, with capacity to restore at a "warm" alternate site. (Silver standard)

Disaster Events and Recent Examples:

- Weather (snow, ice, rain, hurricane, flood, etc.)
    - Ice Storm of 1998 caused widespread outages for over a week.
    - Tropical Storm Irene in 2010 flooded six of Vermont's data centers.
    - Hurricane Sandy in 2012 knocked out internet and cell towers in mid-Atlantic region for many days.

- Cyber attacks (2012)
    - South Carolina: Security breach of revenue data will cost the state $20+ million.
    - Utah: Security breach of half million Social Security numbers.
    - Texas: 3.5 million records exposed.

- Fire

- Earthquake

- Terrorism

- Pandemic flu

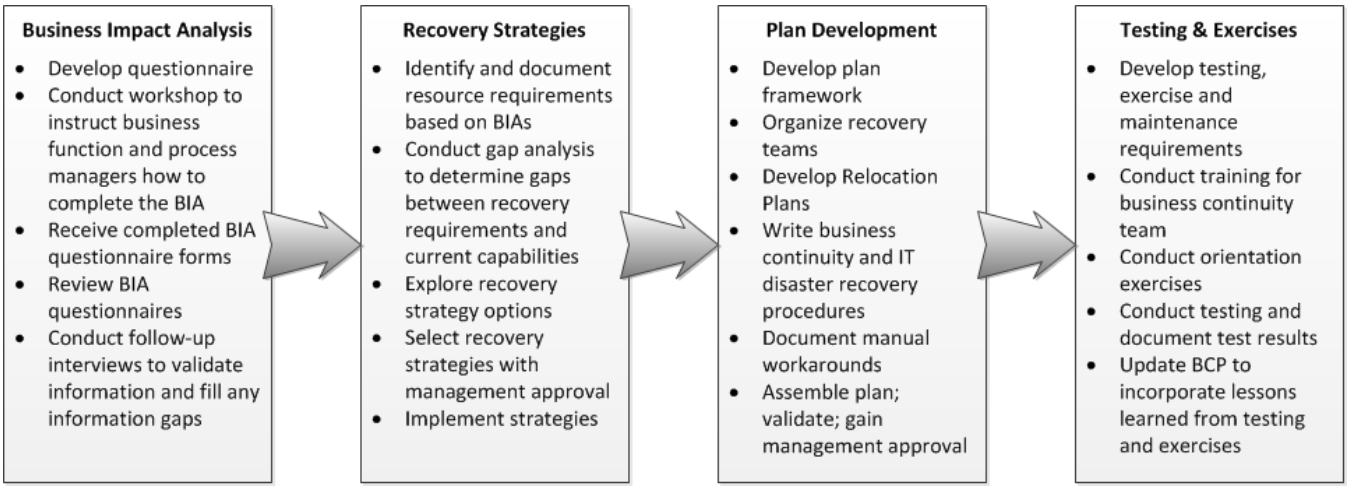
- Electricity grid failure

Section 3: Industry Best Practices

Industry Best Practices:

- **Business Continuity (BC):** Business-critical functions are identified in terms of risk to continuity of business operations, customer base, and revenue.
- **Disaster Recovery (DR):** Disaster recovery capacity for supporting physical and technology infrastructure is viewed as a business investment, necessary to protect the organization's critical operations. Organizations protect business-critical functions by ensuring secondary capacity to continue operations.
- **Time to Recover:** Best practices ensure that business-critical functions and supporting physical and technology infrastructure are recoverable quickly. Time to Recover depends on the level of investment:
    - **High investment:** Critical business functions never go down because there is full redundancy at a "hot" alternate site. (Gold standard)
    - **Moderate investment:** Critical business functions are recoverable within a few hours or days, with capacity to restore at a "warm" alternate site. (Silver standard)

Business continuity planning steps:



(Federal Emergency Management Agency website, www.ready.gov)

Business continuity stages:

1. Business impact analysis (BIA) plan
2. Link into Disaster Recovery plan
3. Annual tests and plan to ensure continuity of business operations

Disaster recovery stages:

1. Identify infrastructure
2. Categorize systems into recovery standards (gold, silver, etc.)
3. Recovery plan for physical and technology resources
4. Annual tests

Current Environment, Future State, and Roadmap (summary)

Topic	Current	Desired	Timeline
Funding and Staff Resources	• Limited funding • No dedicated staff resources for BC/DR	• With agencies, develop plan for adequate investment in BC/DR, built into the agencies' IT budgets and OIT's rates. • OIT hire a BC/DR manager	• Ongoing • Mid 2013
Network, Data Centers, and Other Infrastructure	• Network is redundant between data centers. • Data centers are mostly stand-alone with little fail-over capacity between them. No alternate site for data centers. • Other infrastructure (data storage, etc.) is largely not redundant across sites.	• Data Center: If we lose a data center, be able to automatically fail-over of mission-critical systems to alternate data center. Depending on level of investment, either: o Complete fail-over of all mission-critical systems, with little down-time; or o Partial fail-over of selected mission-critical systems, with varying levels of down-time. • Other infrastructure: Fail-over to alternate location. • Contracts with vendors for potential fail-over to externally hosted data centers and other infrastructure. • Develop 3rd party Cloud strategy.	• End of 2014, subject to availability of funds • TBD • TBD • TBD
BC/DR Planning and Exercises	• No annual plan / exercise.	• Planning and framework for annual DR exercises of mission-critical systems (internal and external hosted). • First mock disaster drill. • Refreshed documentation and inventories.	• End of 2014, subject to availability of funds • End of 2014 • End of 2014
Business Impact Analyses (BIA)	• Twenty percent of systems (400+) have been analyzed. • 600+ more systems need a BIA.	• BIA of all critical business application systems completed and refreshed.	• End of 2014 (quarterly status)

Current Environment, Future State, and Roadmap

Current Environment – Maine:

1. **Funding and Staff Resources:**
   - **Funding:** Industry standard investment (Gartner[1]) in DR is at least 3% of IT budget. The State of Maine, a $3 billion organization, currently has less than 0.5% invested in DR capacity.
   - **Staff Resources:** OIT currently does not have anyone assigned to the BC/DR function full time.

2. **Network, Data Centers, and Other Infrastructure:**
   - **Network:** Over the past two years, the State's network links have been built out to be fully redundant between the two primary data centers. This means that if the network link is lost, it will fail-over to another high-speed link to support communications.
   - **Data Centers:** The State's two major data centers and one small data center host 800 servers and core infrastructure that support the vast majority of application systems for all Executive Branch agencies. If we lose one of the data centers to a fire or water damage, we cannot automatically fail-over to the other. Neither data center has enough spare capacity and existing equipment to completely carry the load of the other data center.
   - **Other Infrastructure:** Other key infrastructure such as the State's e-mail system and central data storage are redundant in the sense of having backup units, but those units are in the same data center – there is no alternate site automatic fail-over capacity.

Current data centers with little fail-over capacity and equipment redundancy
(excess space capacity at each data center = 20-25%, but little extra equipment capacity)

CMCC Data Center
(40% of agency systems)
- Labor, Public Safety, etc.

Sewall Street Data Center
(50% of agency systems)
- DHHS, DEP, etc.

Long-term strategy
(vendor hosting off-site DR capacity)

Footnote 1: Gartner Document Id G0235815, Survey Analysis: IT Disaster Recovery Management Spending and Testing Activities Expanded in 2012, by John P Morency & Kevin Knox, July 18, 2012.

3. **Business Impact Analyses (BIA):**
   - Using a template and formula, each agency application system is scored by five categories of factors to determine the business impact of loss of that system.
     1. Maximum Tolerable Period of Disruption
     2. Asset Value
     3. Importance
     4. Financial Impact (tangible)
     5. Legal & Public Impact (intangible):
   - OIT and the agencies have worked together to complete about 20% (400 systems) of the initial BIAs, but many others have been started. Goal for completion of all is 2014.
   - There has not been any discussion between OIT and the agencies regarding the DR expense of the agencies' desired recovery objectives. Even for the 20% of the BIAs completed, no evaluation has been made for the resources close the gap between current capability and desired capability described in the BIA.

BC/DR Planning and Exercises:

- BC/DR planning and exercises have not been done due to limited staff resources.

- OIT currently assumes the following recovery sequence for business functions. This priority order should be confirmed with the Governor's Office:
  #1 – Core information infrastructure that supports command and control and all state government functions below
  (E-mail, network, data centers, servers, disk storage, etc.)
  #2 – Citizen safety and health
  (Public Safety / State Police systems, Corrections systems, DHHS systems related to health, DEP systems for monitoring air and water quality, DOT systems for highway safety and maintenance)
  #3 – Revenue generating
  (Central tax system, on-line tax filing, one-stop business licensing, on-line hunting and fishing licenses, etc.)
  #4 – Financial services to citizens and internal financial management
  (Unemployment checks, food stamps, child support enforcement, Advantage central accounting system, payroll, etc.)
  #5 – Financial services to providers and contractors
  (Medicaid claims, payments to contractors, etc.)
  #6 – Regulatory
  (Environmental protection, Education systems, professional and financial licensing, etc.)
  #7 – All other government functions and services
  (Hundreds of systems across many agencies)

- A complete inventory does not currently exist to link the hundreds of agency application systems to the seven recovery categories above.

- No unified evaluation regarding DR plans for remotely-hosted applications.

Future State:

1. **Funding and Staff Resources:**
    - With agencies, plan adequate investment in BC/DR, built into the agencies' IT budgets and OIT's rates. Of the Statewide IT budget of $143 million a year, at least 3% ($4 million or more) should be set-aside for better BC/DR capacity.
    - Assign adequate staff resources to the BC/DR function (both in OIT and the agencies) to give it proper focus and priority.

2. **Network, Data Centers, and Other Infrastructure:**
    - In the event of loss of a data center, we should be able to automatically fail-over to another data center (either internally or externally hosted) in order to continue critical business operations for Maine State Government.
    - With different levels of investment, this continuity of operations would either be:
        - Complete fail-over of all mission-critical systems, with little or no down-time.
        - Partial fail-over of selected mission-critical systems, with varying levels of down-time
        - Adoption of 3rd party, cloud based solution

3. **Business Impact Analysis (BIA):**
    - Business impact analysis of critical business application systems (completed and refreshed)

4. **BC/DR Planning and Exercises:**
    - Annual exercises and refreshed documentation for testing our DR capacity for:
        - Data centers
        - Network
        - Other core infrastructure such as data storage
        - Critical business application systems (both OIT-hosted and externally-hosted)
        - Critical office locations
    - Inventory of critical business application systems and core infrastructure.
    - Completed and continuously updated plans and exercises in place.
    - Contracts with vendors for potential fail-over to externally hosted data centers.

Timeframe – Roadmap (2013-2014):

1. **Funding and Staff Resources:**
    - Annually: As part of each year's budget for IT, work with agencies to look for ways to build in BC/DR capacity for their mission-critical business systems. Since OIT does not have its own budget but uses an internal fee-for-service fund, Agencies' willingness to make greater investment in BC/DR capacity depends partly on their awareness of the risk they now face, as documented in the set of partially completed business impact analyses (BIAs).
    - Mid-2013: Funds allocated to recruit a full-time OIT BC/DR Manager.

2. **Network, Data Centers, and Other Infrastructure:**
    - End of 2013: The OIT DR Manager will facilitate estimating the BC/DR capacities of both OIT data centers.
    - End of 2014 (subject to availability of funds): OIT will ensure completely automated failover of mission-critical systems between the two primary data centers. This will require both technical work, as well as a greater investment in equipment capacity.
    - End of 2014 (subject to availability of funds): Contracts with vendors for potential fail-over to externally hosted data centers.

3. **Business Impact Analyses (BIA):**
    - End of 2014: Through the growing set of BIAs, OIT will provide DR cost estimates to the agencies, in order to satisfy their needs for recoverability of each system. Based on these estimates, Agencies may adjust their BC/DR expectations to what they can realistically afford.
    - End of 2014 (quarterly milestone check): OIT and the agencies will continue to complete and update the BIA for all agency-critical business application systems.

4. **BC/DR Planning and Exercises:**
    - End of 2013: Inventory of critical business application systems and core infrastructure updated (and refreshed quarterly).
    - End of 2014: Completed and continuously updated plans and exercises in place.
    - Annually: The OIT DR Manager will facilitate the DR plan, for both OIT-hosted and remotely-hosted applications. The OIT DR Manager will facilitate annual DR exercise for OIT-hosted applications.
    - Annually: The OIT DR Manager will hold remote-hosting vendors accountable regarding their DR plans and recovery exercise results.

5. **Third party, independent review of State of Maine BC / DR readiness**
    - End of 2014

See Appendix for four potential disaster events, detailing agency business impact, technology impact, and time to recover.

Appendix

Disaster events – Examples:

Loss of governmental functions or computer systems may occur due to events such as:

1. **Data Center fire or other destruction:**
   - **Agency Business Impact:**
     - Depending on which data center is down and for how long, both critical and non-critical governmental functions could be impacted for up to half of State Government Agencies.
     - Agencies might not have access to critical data, such as for police checking criminal history at a traffic stop, background on families social workers are visiting, and hundreds of other databases that could be down for extended periods.
     - For citizen services, agencies would have to implement their business continuity plans for manual processing of transactions such as welfare checks.
   - **Technology Impact:**
     - Crippling up to half of the State's network, disk storage, and hundreds of agency application systems and databases, and potentially e-mail State-wide.
   - **Time to <u>fully</u> restore: 3-5 months.**
     - May be able to restore 25% of systems and functions within less than 1 month; 50% within 2-3 months; and 75% within 4-5 months.

2. **Agency building fire or other destruction:**
   - **Agency Business Impact:**
     - Preventing Agency staff from conducting normal governmental operations and delivering citizen services.
     - Staff would have to be moved to another building to resume operations there. They would use manual processing until their computers were replaced.
   - **Technology Impact:**
     - Need to replace desktop computers. However, most data is stored on the servers in the data center, not on the desktop computers at the Agency building.
     - E-mail is unaffected since it is hosted at the data center, not at the Agency building.
   - **Time to <u>fully</u> restore: 4 weeks.**

3. **Cyber attack (computer hackers):**
   - **Agency Business Impact:**
     - The impact would depend on the nature of the cyber attack, which could be intrusion, theft, destruction, or corruption of databases.
   - **Technology Impact:**
     - Intrusion, theft, destruction, or corruption of critical or personally sensitive databases, the impact of which is often uncertain and difficult to recover from.
   - **Time to <u>fully</u> restore: 2-5 days.**

4. **Any event preventing large numbers of people from coming to work (like a pandemic health outbreak or a major weather event like the Ice Storm 1998)**
    - **Agency Business Impact:**
        - Preventing large numbers of people from coming to work. This may mean either much-reduced level of operations and citizen services, or even temporary closing of office locations.
    - **Technology Impact:**
        - The staff wouldn't have access to their computers at the workplace, but could be set up with remote access and laptops computers to be able to work from home, if they have higher-speed Internet access at home.
    - **Time to <u>fully</u> restore: 4 weeks**
        - The amount of time to set up large numbers of people with remote access and laptop computers for working at home.